ICS 35.040
L 80
备案号:36830—2012

GM

中华人民共和国密码行业标准

GM/T 0003.5—2012

SM2 椭圆曲线公钥密码算法 第5部分:参数定义

Public key cryptographic algorithm SM2 based on elliptic curves—
Part 5:Parameter definition

2012-03-21 发布 2012-03-21 实施

国家密码管理局 发布

VISIT…

LANZAROTE
Caliente.COM

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　参数定义 …… 1
附录 A（资料性附录）　数字签名与验证示例 …… 2
　A.1　一般要求 …… 2
　A.2　SM2 椭圆曲线数字签名 …… 2
附录 B（资料性附录）　密钥交换及验证示例 …… 4
　B.1　一般要求 …… 4
　B.2　SM2 椭圆曲线密钥交换协议 …… 4
附录 C（资料性附录）　消息加解密示例 …… 8
　C.1　一般要求 …… 8
　C.2　SM2 椭圆曲线消息加解密 …… 8

前　　言

GM/T 0003　2012《SM2 椭圆曲线公钥密码算法》分为 5 个部分：

- 第 1 部分：总则；
- 第 2 部分：数字签名算法；
- 第 3 部分：密钥交换协议；
- 第 4 部分：公钥加密算法；
- 第 5 部分：参数定义。

本部分为 GM/T 0003 的第 5 部分。

本部分依据 GB/T 1.1　2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分的附录 A、附录 B 和附录 C 为资料性附录。

本部分由国家密码管理局提出并归口。

本部分起草单位：北京华大信安科技有限公司、中国人民解放军信息工程大学、中国科学院数据与通信保护研究教育中心。

本部分主要起草人：陈建华、祝跃飞、叶顶峰、胡磊、裴定一、彭国华、张亚娟、张振峰。

SM2 椭圆曲线公钥密码算法
第 5 部分：参数定义

1 范围

GM/T 0003 的本部分规定了 SM2 椭圆曲线公钥密码算法的曲线参数，并给出了数字签名与验证、密钥交换与验证、消息加解密示例。

2 参数定义

SM2 使用素数域 256 位椭圆曲线。

椭圆曲线方程：$y^2 - x^3 + ax + b$

曲线参数：

p—FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF

a—FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC

b—28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93

n—FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123

x_G—32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7

y_G—BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0

附 录 A
（资料性附录）
数字签名与验证示例

A.1 一般要求

本附录选用 GM/T 0004　2012《SM3 密码杂凑算法》给出的密码杂凑函数，其输入是长度小于 2^{64} 的消息比特串，输出是长度为 256 比特的杂凑值，记为 $H_{256}(\ )$。

本附录中，所有用 16 进制表示的数，左边为高位，右边为低位。

本附录中，消息采用 ASCII 编码。

设 ID_A 的 ASCII 编码为：31323334 35363738 31323334 35363738。$ENTL_A-0080$。

A.2 SM2 椭圆曲线数字签名

椭圆曲线方程为：y^2-x^3+ax+b

示例：F_p-256

素数 p：FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF

系数 a：FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC

系数 b：28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93

基点 G　(x_G,y_G)，其阶记为 n。

坐标 x_G：32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7

坐标 y_G：BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0

阶 n：　FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123

待签名的消息 M：message digest

M 的 ASCII 码表示为：6D65737361676520646967657374

私钥 d_A：3945208F 7B2144B1 3F36E38A C6D39F95 88939369 2860B51A 42FB81EF 4DF7C5B8

公钥 P_A　(x_A, y_A)：

坐标 x_A：09F9DF31 1E5421A1 50DD7D16 1E4BC5C6 72179FAD 1833FC07 6BB08FF3 56F35020

坐标 y_A：CCEA490C E26775A5 2DC6EA71 8CC1AA60 0AED05FB F35E084A 6632F607 2DA9AD13

杂凑值 Z_A　$H_{256}(ENTL_A \| ID_A \| a \| b \| x_G \| y_G \| x_A \| y_A)$。

Z_A：B2E14C5C 79C6DF5B 85F4FE7E D8DB7A26 2B9DA7E0 7CCB0EA9 F4747B8C CDA8A4F3

签名各步骤中的有关值：

$\overline{M}$　$Z_A \| M$：

B2E14C5C 79C6DF5B 85F4FE7E D8DB7A26 2B9DA7E0 7CCB0EA9 F4747B8C CDA8A4F3
6D657373 61676520 64696765 7374

密码杂凑函数值 e　$H_{256}(\overline{M})$：F0B43E94 BA45ACCA ACE692ED 534382EB 17E6AB5A 19CE7B31 F4486FDF C0D28640

产生随机数 k：59276E27 D506861A 16680F3A D9C02DCC EF3CC1FA 3CDBE4CE 6D54B80D EAC1BC21

计算椭圆曲线点 (x_1, y_1)　$[k]G$：

坐标 x_1：04EBFC71 8E8D1798 62043226 8E77FEB6 415E2EDE 0E073C0F 4F640ECD 2E149A73

坐标 y_1：E858F9D8 1E5430A5 7B36DAAB 8F950A3C 64E6EE6A 63094D99 283AFF76 7E124DF0

计算 r　$(e+x_1)\bmod n$：F5A03B06 48D2C463 0EEAC513 E1BB81A1 5944DA38 27D5B741 43AC7EAC EEE720B3

$(1+d_A)^{-1}$：4DFE9D9C 1F5901D4 E6F58E4E C3D04567 822D2550 F9B88E82 6D1B5B3A B9CD0FE0

计算 $s\ \ ((1+d_A)\ ^{1}(k-rd_A))\mathrm{mod}n$：B1B6AA29 DF212FD8 763182BC 0D421CA1 BB9038FD 1F7F42D4 840B69C4 85BBC1AA

消息 M 的签名为 (r,s)：

值 r：F5A03B06 48D2C463 0EEAC513 E1BB81A1 5944DA38 27D5B741 43AC7EAC EEE720B3

值 s：B1B6AA29 DF212FD8 763182BC 0D421CA1 BB9038FD 1F7F42D4 840B69C4 85BBC1AA

验证各步骤中的有关值：

密码杂凑函数值 $e'\ \ H_{256}(\overline{M'})$：F0B43E94 BA45ACCA ACE692ED 534382EB 17E6AB5A 19CE7B31 F4486FDF C0D28640

计算 $t\ \ (r'+s')\mathrm{mod}n$：A756E531 27F3F43B 851C47CF EEFD9E43 A2D133CA 258EF4EA 73FBF468 3ACDA13A

计算椭圆曲线点 $(x'_0, y'_0)\ \ [s']G$：

坐标 x'_0：2B9CE14E 3C8D1FFC 46D693FA 0B54F2BD C4825A50 6607655D E22894B5 C99D3746

坐标 y'_0：277BFE04 D1E526B4 E1C32726 435761FB CE0997C2 6390919C 4417B3A0 A8639A59

计算椭圆曲线点 $(x'_{00}, y'_{00})\ \ [t]P_A$：

坐标 x'_{00}：FDAC1EFA A770E463 5885CA1B BFB360A5 84B238FB 2902ECF0 9DDC935F 60BF4F9B

坐标 y'_{00}：B89AA926 3D5632F6 EE82222E 4D63198E 78E095C2 4042CBE7 15C23F71 1422D74C

计算椭圆曲线点 $(x_1', y_1')\ \ [s']G+[t]P_A$：

坐标 x'_1：04EBFC71 8E8D1798 62043226 8E77FEB6 415E2EDE 0E073C0F 4F640ECD 2E149A73

坐标 y'_1：E858F9D8 1E5430A5 7B36DAAB 8F950A3C 64E6EE6A 63094D99 283AFF76 7E124DF0

计算 $R\ \ (e'+x'_1)\mathrm{mod}n$：F5A03B06 48D2C463 0EEAC513 E1BB81A1 5944DA38 27D5B741 43AC7EAC EEE720B3

附　录　B
（资料性附录）
密钥交换及验证示例

B.1　一般要求

本附录选用 GM/T 0004　2012《SM3 密码杂凑算法》给出的密码杂凑函数，其输入是长度小于 2^{64} 的消息比特串，输出是长度为 256 比特的杂凑值，记为 H_{256}( )。

本附录中，所有用 16 进制表示的数，左边为高位，右边为低位。

设 ID_A 的 ASCII 编码为：31323334 35363738 31323334 35363738。$ENTL_A$－0080。

设 ID_B 的 ASCII 编码为：31323334 35363738 31323334 35363738。$ENTL_B$－0080。

B.2　SM2 椭圆曲线密钥交换协议

椭圆曲线方程为：$y^2 - x^3 + ax + b$

示例：F_p－256

素数 p：FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF

系数 a：FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC

系数 b：28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93

余因子 h：1

基点 G　(x_G, y_G)，其阶记为 n。

坐标 x_G：32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7

坐标 y_G：BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0

阶 n：　FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123

用户 A 的私钥 d_A：81EB26E9 41BB5AF1 6DF11649 5F906952 72AE2CD6 3D6C4AE1 678418BE 48230029

用户 A 的公钥 P_A　(x_A, y_A)：

坐标 x_A：160E1289 7DF4EDB6 1DD812FE B96748FB D3CCF4FF E26AA6F6 DB9540AF 49C94232

坐标 y_A：4A7DAD08 BB9A4595 31694BEB 20AA489D 6649975E 1BFCF8C4 741B78B4 B223007F

用户 B 的私钥 d_B：78512991 7D45A9EA 5437A593 56B82338 EAADDA6C EB199088 F14AE10D EFA229B5

用户 B 的公钥 P_B　(x_B, y_B)：

坐标 x_B：6AE848C5 7C53C7B1 B5FA99EB 2286AF07 8BA64C64 591B8B56 6F7357D5 76F16DFB

坐标 y_B：EE489D77 1621A27B 36C5C799 2062E9CD 09A92643 86F3FBEA 54DFF693 05621C4D

杂凑值 Z_A　$H_{256}(ENTL_A \| ID_A \| a \| b \| x_G \| y_G \| x_A \| y_A)$。

Z_A：3B85A571 79E11E7E 513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1

杂凑值 Z_B　$H_{256}(ENTL_B \| ID_B \| a \| b \| x_G \| y_G \| x_B \| y_B)$。

Z_B：79C988D6 3229D97E F19FE02C A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7

密钥交换 A1—A3 步骤中的有关值：

产生随机数 r_A：D4DE1547 4DB74D06 491C440D 305E0124 00990F3E 390C7E87 153C12DB 2EA60BB3

计算椭圆曲线点 R_A　$[r_A]G$　(x_1, y_1)：

坐标 x_1：64CED1BD BC99D590 049B434D 0FD73428 CF608A5D B8FE5CE0 7F150269 40BAE40E

坐标 y_1：376629C7 AB21E7DB 26092249 9DDB118F 07CE8EAA E3E7720A FEF6A5CC 062070C0

密钥交换 B1—B9 步骤中的有关值：

产生随机数 r_B：7E071248 14B30948 9125EAED 10111316 4EBF0F34 58C5BD88 335C1F9D 596243D6

计算椭圆曲线点 R_B $[r_B]G$ (x_2, y_2):

坐标 x_2:ACC27688 A6F7B706 098BC91F F3AD1BFF 7DC2802C DB14CCCC DB0A9047 1F9BD707

坐标 y_2:2FEDAC04 94B2FFC4 D6853876 C79B8F30 1C6573AD 0AA50F39 FC87181E 1A1B46FE

取 $\overline{x}_2$ $2^{127}+(x_2\&(2^{127}-1))$:FDC2802C DB14CCCC DB0A9047 1F9BD707

计算 t_B $(d_B+\overline{x}_2\cdot r_B)\bmod n$:

D0429637 F5A6D5D1 E6C54523 5169DF85 23116306 0A654ECB A0F657FD 629E8DD9

取 $\overline{x}_1$ $2^{127}+(x_1\&(2^{127}-1))$:CF608A5D B8FE5CE0 7F150269 40BAE40E

计算椭圆曲线点$[\overline{x}_1]R_A$ (x_{A0}, y_{A0}):

坐标 x_{A0}:8D62DAF7 DC084E4A 85D32214 68605854 5837BDC2 2D6E9AFE 015828A8 E1094EC2

坐标 y_{A0}:564DC0FA 639B2967 E65F3448 CA06627E F3FE67C2 1561C5BE BB399552 29A84760

计算椭圆曲线点 $P_A+[\overline{x}_1]R_A$ (x_{A1}, y_{A1}):

坐标 x_{A1}:85C40F88 CECA80E3 8172093F C4BA4581 88E7C58A F81CF2AF 454EC431 43E55615

坐标 y_{A1}:8C152CB0 A131C958 C279DEBE CC6AB739 6A7BC875 FC801BB2 94C284F4 7F65F6ED

计算 V $[h\cdot t_B](P_A+[\overline{x}_1]R_A)$ (x_V, y_V):

坐标 x_V:C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F

坐标 y_V:3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7

计算 K_B $KDF(x_V \| y_V \| Z_A \| Z_B, klen)$:

$x_V \| y_V \| Z_A \| Z_B$:

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3252B35B
191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7 3B85A571 79E11E7E
513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E F19FE02C
A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7

$klen$ 128

共享密钥 K_B:6C893473 54DE2484 C60B4AB1 FDE4C6E5

计算选项 S_B $Hash(0x02 \| y_V \| Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2))$:

$x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2$:

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3B85A571
79E11E7E 513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E
F19FE02C A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7 64CED1BD BC99D590 049B434D
0FD73428 CF608A5D B8FE5CE0 7F150269 40BAE40E 376629C7 AB21E7DB 26092249 9DDB118F
07CE8EAA E3E7720A FEF6A5CC 062070C0 ACC27688 A6F7B706 098BC91F F3AD1BFF 7DC2802C
DB14CCCC DB0A9047 1F9BD707 2FEDAC04 94B2FFC4 D6853876 C79B8F30 1C6573AD 0AA50F39
FC87181E 1A1B46FE

$Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$:

90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

$0x02 \| y_V \| Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$:

02 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7
90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

选项 S_B:D3A0FE15 DEE185CE AE907A6B 595CC32A 266ED7B3 367E9983 A896DC32 FA20F8EB

密钥交换 A4—A10 步骤中的有关值:

取 $\overline{x}_1$ $2^{127}+(x_1\&(2^{127}-1))$:CF608A5D B8FE5CE0 7F150269 40BAE40E

计算 t_A $(d_A+\overline{x}_1\cdot r_A)\bmod n$:3D68C0C0 6DC40F17 B9DDFE00 93D3C0E4 969ED112 4A187FA8 AD02F81E 3C11CCE6

取 $\overline{x}_2$ $2^{127}+(x_2\&(2^{127}-1))$:FDC2802C DB14CCCC DB0A9047 1F9BD707

计算椭圆曲线点$[\overline{x}_2]R_B$ (x_{B0}, y_{B0}):

坐标 x_{B0}:DA68EF84 FE616D92 438BBE69 BCC52DB9 CE5CBEA9 93944CBC 331BA26D 6082E912

坐标 y_{B0}:4831E862 898B4356 32D8FFA0 1869CD65 645822BD D3B4E9E0 46BCAB85 6F02F110

计算椭圆曲线点 $P_B+[\overline{x}_2]R_B$ (x_{B1}, y_{B1}):

坐标 x_{B1}:FE7C111C C3E628E3 FE709DF2 E6E331CD C2A3A30E EA0CDC3C D10C0759 EAB15199

坐标 y_{B1}:12D6F496 361948C9 EC67E603 DF93C008 86EFAEEA C591C2D5 D16B67F2 FE1AD77E

计算 U $[h\cdot t_A](P_B+[\overline{x}_2]R_B)$ (x_U,y_U):

坐标 x_U:C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F

坐标 y_U:3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7

计算 K_A $KDF(x_U \parallel y_U \parallel Z_A \parallel Z_B, klen)$:

$x_U \parallel y_U \parallel Z_A \parallel Z_B$:

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3252B35B
191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7 3B85A571 79E11E7E
513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E F19FE02C
A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7

$klen$ 128

共享密钥 K_A:6C893473 54DE2484 C60B4AB1 FDE4C6E5

计算选项 S_1 $Hash(0x02 \parallel y_U \parallel Hash(x_U \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2))$:

$x_U \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2$:

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3B85A571
79E11E7E 513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E
F19FE02C A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7 64CED1BD BC99D590 049B434D
0FD73428 CF608A5D B8FE5CE0 7F150269 40BAE40E 376629C7 AB21E7DB 26092249 9DDB118F
07CE8EAA E3E7720A FEF6A5CC 062070C0 ACC27688 A6F7B706 098BC91F F3AD1BFF 7DC2802C
DB14CCCC DB0A9047 1F9BD707 2FEDAC04 94B2FFC4 D6853876 C79B8F30 1C6573AD 0AA50F39
FC87181E 1A1B46FE

$Hash(x_U \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2)$:90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B
627D4F4D D047B7F6

$0x02 \parallel y_U \parallel Hash(x_U \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2)$:

02 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7
90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

选项 S_1:D3A0FE15 DEE185CE AE907A6B 595CC32A 266ED7B3 367E9983 A896DC32 FA20F8EB

计算选项 S_A $Hash(0x03 \parallel y_U \parallel Hash(x_U \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2))$:

$x_U \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2$:

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3B85A571
79E11E7E 513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E
F19FE02C A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7 64CED1BD BC99D590 049B434D
0FD73428 CF608A5D B8FE5CE0 7F150269 40BAE40E 376629C7 AB21E7DB 26092249 9DDB118F
07CE8EAA E3E7720A FEF6A5CC 062070C0 ACC27688 A6F7B706 098BC91F F3AD1BFF 7DC2802C
DB14CCCC DB0A9047 1F9BD707 2FEDAC04 94B2FFC4 D6853876 C79B8F30 1C6573AD 0AA50F39
FC87181E 1A1B46FE

$Hash(x_U | Z_A | Z_B | x_1 | y_1 | x_2 | y_2)$:90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B
627D4F4D D047B7F6

$0x03 \parallel y_U \parallel Hash(x_U \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2)$:

03 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7
90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

选项 S_A:18C7894B 3816DF16 CF07B05C 5EC0BEF5 D655D58F 779CC1B4 00A4F388 4644DB88

密钥交换 B10 步骤中的有关值:

计算选项 S_2 $Hash(0x03 \parallel y_V \parallel Hash(x_V \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2))$:

$x_V \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2$:

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3B85A571

79E11E7E 513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E
F19FE02C A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7 64CED1BD BC99D590 049B434D
0FD73428 CF608A5D B8FE5CE0 7F150269 40BAE40E 376629C7 AB21E7DB 26092249 9DDB118F
07CE8EAA E3E7720A FEF6A5CC 062070C0 ACC27688 A6F7B706 098BC91F F3AD1BFF 7DC2802C
DB14CCCC DB0A9047 1F9BD707 2FEDAC04 94B2FFC4 D6853876 C79B8F30 1C6573AD 0AA50F39
FC87181E 1A1B46FE

$Hash(x_V | Z_A | Z_B | x_1 | y_1 | x_2 | y_2)$：90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B
627D4F4D D047B7F6

$0x03 \| y_V \| Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$：

03 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7
90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

选项 S_2：18C7894B 3816DF16 CF07B05C 5EC0BEF5 D655D58F 779CC1B4 00A4F388 4644DB88

附 录 C
（资料性附录）
消息加解密示例

C.1 一般要求

本附录选用 GM/T 0004 2012《SM3 密码杂凑算法》给出的密码杂凑函数，其输入是长度小于 2^{64} 的消息比特串，输出是长度为 256 比特的杂凑值，记为 $H_{256}(\ )$。

本附录中，所有用 16 进制表示的数，左边为高位，右边为低位。

本附录中，明文采用 ASCII 编码。

C.2 SM2 椭圆曲线消息加解密

椭圆曲线方程为：$y^2 - x^3 + ax + b$

示例：$F_p - 256$

素数 p：FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF

系数 a：FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC

系数 b：28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93

基点 G (x_G, y_G)，其阶记为 n。

坐标 x_G：32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7

坐标 y_G：BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0

阶 n：　FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123

待加密的消息 M：encryption standard

消息 M 的 16 进制表示：656E63 72797074 696F6E20 7374616E 64617264

私钥 d_B：3945208F 7B2144B1 3F36E38A C6D39F95 88939369 2860B51A 42FB81EF 4DF7C5B8

公钥 P_B (x_B, y_B)为：

坐标 x_B：09F9DF31 1E5421A1 50DD7D16 1E4BC5C6 72179FAD 1833FC07 6BB08FF3 56F35020

坐标 y_B：CCEA490C E26775A5 2DC6EA71 8CC1AA60 0AED05FB F35E084A 6632F607 2DA9AD13

加密各步骤中的有关值：

产生随机数 k：59276E27 D506861A 16680F3A D9C02DCC EF3CC1FA 3CDBE4CE 6D54B80D EAC1BC21

计算椭圆曲线点 C_1 $[k]G$ (x_1, y_1)：

坐标 x_1：04EBFC71 8E8D1798 62043226 8E77FEB6 415E2EDE 0E073C0F 4F640ECD 2E149A73

坐标 y_1：E858F9D8 1E5430A5 7B36DAAB 8F950A3C 64E6EE6A 63094D99 283AFF76 7E124DF0

在此 C_1 选用未压缩的表示形式，点转换成字节串的形式为 $PC \| x_1 \| y_1$，其中 PC 为单一字节且 PC 04，仍记为 C_1。

计算椭圆曲线点$[k]P_B$ (x_2, y_2)：

坐标 x_2：335E18D7 51E51F04 0E27D468 138B7AB1 DC86AD7F 981D7D41 6222FD6A B3ED230D

坐标 y_2：AB743EBC FB22D64F 7B6AB791 F70658F2 5B48FA93 E54064FD BFBED3F0 BD847AC9

消息 M 的比特长度 $klen$ 152

计算 t $KDF(x_2 \| y_2, klen)$：44E60F DBF0BAE8 14376653 74BEF267 49046C9E

计算 C_2 $M \oplus t$：21886C A989CA9C 7D580873 07CA9309 2D651EFA

计算 C_3 $Hash(x_2 \| M \| y_2)$：

$x_2 \| M \| y_2$：

335E18D7 51E51F04 0E27D468 138B7AB1 DC86AD7F 981D7D41 6222FD6A B3ED230D

656E6372 79707469 6F6E2073 74616E64 617264AB 743EBCFB 22D64F7B 6AB791F7
0658F25B 48FA93E 54064FDB FBED3F0B D847AC9

C_3:59983C18 F809E262 923C53AE C295D303 83B54E39 D609D160 AFCB1908 D0BD8766

输出密文 $M \quad C_1 \| C_3 \| C_2$:

04 04EBFC71 8E8D1798 62043226 8E77FEB6 415E2EDE 0E073C0F 4F640ECD 2E149A73
E858F9D8 1E5430A5 7B36DAAB8F950A3C 64E6EE6A 63094D99 283AFF76 7E124DF0
59983C18 F809E262 923C53AE C295D303 83B54E39 D609D160 AFCB1908 D0BD8766
21886CA9 89CA9C7D 58087307 CA93092D 651EFA

解密各步骤中的有关值:

计算椭圆曲线点$[d_B]C_1 \quad (x_2, y_2)$:

坐标 x_2:335E18D7 51E51F040 E27D4681 38B7AB1D C86AD7F9 81D7D416 222FD6AB 3ED230D

坐标 y_2:AB743EBC FB22D64F 7B6AB791 F70658F2 5B48FA93 E54064FD BFBED3F0 BD847AC9

计算 $t \quad KDF(x_2 \| y_2, klen)$:44E60F DBF0BAE8 14376653 74BEF267 49046C9E

计算 $M' \quad C_2 \oplus t$:656E63 72797074 696F6E20 7374616E 64617264

计算 $u \quad Hash(x_2 \| M' \| y_2)$:

59983C18 F809E262 923C53AE C295D303 83B54E39 D609D160 AFCB1908 D0BD8766

明文 M':656E63 72797074 696F6E20 7374616E 64617264,即为:encryption standard

GM/T 0003.5—2012

中 华 人 民 共 和 国 密 码
行 业 标 准
SM2 椭圆曲线公钥密码算法
第 5 部分：参数定义
GM/T 0003.5—2012

*

中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)

网址 www.spc.net.cn
总编室：(010)64275323　发行中心：(010)51780235
读者服务部：(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16　印张 1　字数 19 千字
2012 年 8 月第一版　2012 年 8 月第一次印刷

*

书号：155066・2-23737　定价 18.00 元

如有印装差错　由本社发行中心调换
版权专有　侵权必究
举报电话：(010)68510107

GM/T 0003.5-2012